Department for Digital, Culture, Media & Sport

Ipsos MORI

Cyber Security Breaches Survey 2020

Education institutions findings annex

This annex includes findings from the small samples of education institutions included for the first time in this year's Cyber Security Breaches Survey. The results cover:

- primary schools
- secondary schools
- further education colleges and universities (which are combined in the reporting).

It supplements a main statistical release by the Department for Digital, Culture, Media and Sport (DCMS), covering the 2020 results for businesses and charities. It can be found on the GOV.UK website, alongside infographic summaries of the findings, at: https://www.gov.uk/government/collections/cyber-security-breaches-survey.

There is another annex, available on the same GOV.UK page, that provides the technical details of the study and copies of the main survey instruments to aid interpretation of the findings.

The Cyber Security Breaches Survey is a quantitative and qualitative study of UK, primarily of businesses and charities. This year's survey includes results for education institutions for the first time.

The survey helps these organisations to understand the nature and significance of the cyber security threats they face, and what others are doing to stay secure. It also supports the government to shape future policy in this area.

For this latest release, the quantitative survey was carried out in winter 2019.

Responsible analyst:

Emma Johns
07990602870

Statistical enquiries:

cyber.survey@culture.gov.uk
@DCMSinsight

General enquiries:

enquiries@culture.gov.uk

Media enquiries:

020 7211 2210

Contents

Chapter 1: Overview of the data

1.1 Summary of methodology

The survey of education institutions comprised a random probability telephone survey, carried out from 9 October 2019 to 23 December 2019. It included:

- 108 primary schools in England (dealing with children aged 5 to 11)
- 72 secondary schools in England (dealing with children aged 11+)
- 8 further education colleges in England and 27 UK universities (reported as one group).

The school samples include free schools, academies, Local Authority-maintained schools and special schools.

1.2 Comparability to the main results for businesses and charities

The education samples this year were intended to be experimental, to see if future surveys including larger samples would be feasible and learning lessons about the best ways to carry out these surveys. As such this part of the survey was on a much smaller scale than the main survey of businesses (1,348 surveyed) and charities (337 surveyed). There is also a qualitative element in the main study, but education institutions were not included in this element. This reflects that businesses and charities are still the main audiences for this survey series.

In this report, we have primarily compared our three education institution samples against each other, and against the benchmark set by UK businesses. The report is intended to give a broad indication, potentially to explore further in new research, of where schools, colleges and universities lie in relation to businesses when it comes to cyber security. This comparison is not subject to statistical significance testing given the very small sample sizes.

1.3 A note on representativeness

The education institution samples are unweighted. They were surveyed as simple random samples, with no stratification.

With this in mind, the primary and secondary school samples might be considered as broadly representative. However, with the achieved samples being relatively small compared to the size of their populations, we believe the results are best treated as indicative. They are unlikely to represent the full variation within these populations.

The further education college and university sample is extremely small (35 interviews) and merges together two independent populations in a way that does not reflect the balance of further education colleges vs. universities. This was done to produce a larger sample size that allows for better deidentification of the data and better indicative analysis. However, it means that the results from this sample should be considered as highly indicative and not representative. They give a broad insight into these two populations and how they might compare against UK businesses.

It is important to remember that our school samples and the sample of further education colleges come from England only (i.e. not including Wales, Scotland or Northern Ireland). This reflects the fact that education policy is devolved across the UK – and the database we used for sampling the school and college populations was the England-only Get information about schools[1] government database.

[1] See https://get-information-schools.service.gov.uk/.

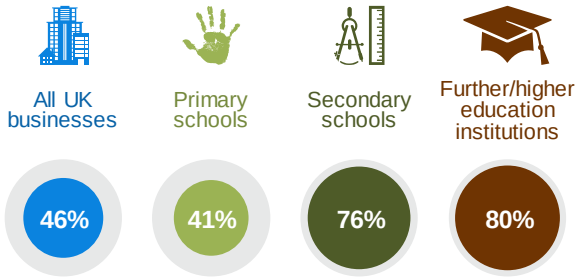
Chapter 2: Key findings

2.1 Incidence and impact of cyber security breaches or attacks

It is important to remember that the survey can only measure the breaches or attacks that organisations have themselves identified. There are likely to be hidden attacks, and others that go unidentified, so the findings reported here may underestimate the full extent of the problem.

Our sample of secondary schools and further and higher education institutions are much more likely to have identified any cyber security breaches or attacks in the last 12 months than the typical business (Figure 2.1). This puts them in line with large businesses (75% identified any breaches or attacks). By contrast, primary schools are in line with micro businesses (43% of whom identified breaches or attacks).

Figure 2.1: Percentage of organisations that have identified breaches or attacks in the last 12 months



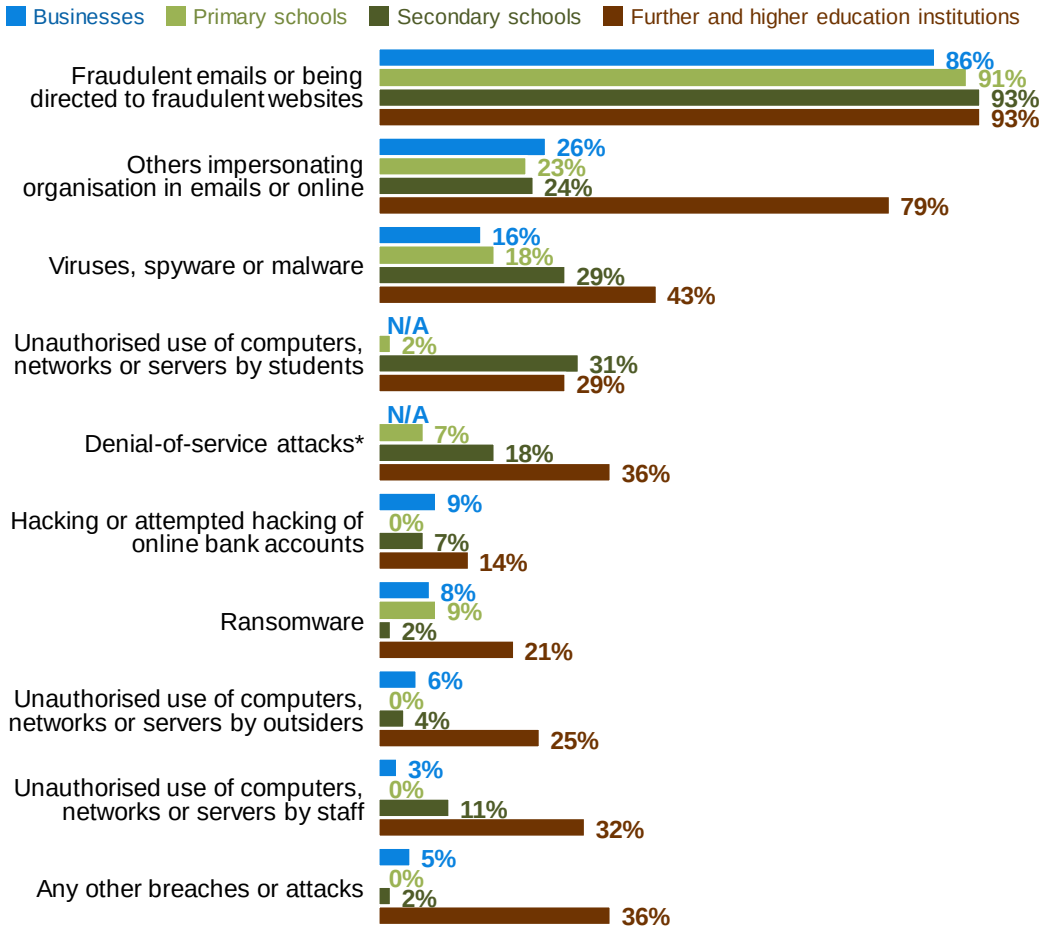
Bases: 1,348 UK businesses; 108 primary schools; 72 secondary schools; 35 further and higher education institutions

The findings reported in the rest of Section 2.1 are based only on the institutions that experienced breaches or attacks. This means that the sample sizes are extremely low.

In the further and higher education sample, there are 28 organisations that experienced breaches or attacks. We cannot put a defined margin of error on samples this small. However, it is worth noting that this group potentially experiences a much broader array of breaches and attacks than primary and secondary schools, as Figure 2.2 suggests. A third (36%) of these institutions say they have experienced different breaches or attacks that are not defined in our survey.

These data also highlight that breaches resulting from student behaviour can be a significant problem for secondary schools and further and higher education institutions to deal with.

Figure 2.2: Percentage that have identified the following types of breaches or attacks in the last 12 months, among the education institutions that have identified any breaches or attacks



Bases: 748 businesses that identified a breach or attack in the last 12 months; 44 primary schools; 55 secondary schools; 28 further and higher education institutions
*This category was omitted from the script for this year's business survey.

Among those that have experienced breaches or attacks in the last 12 months, further and higher education institutions appear to be more severely affected by them – compared to both other education institutions and to the average UK business:

- A total of 54 per cent identified breaches or attacks at least once a week (vs. 11% of primary schools, 13% of secondary schools and 32% of UK businesses).
- A similar proportion (57%) had a material outcome from these breaches, such as a loss of money or data (vs. 23% of primary schools, 32% of secondary schools and 19% of UK businesses). The most common impacts cited by further and higher education institutions are a temporary loss of network access, and the loss or destruction of personal data.
- Four-fifths (82%) were negatively impacted, most commonly in terms of requiring new measures following the breach, having staff time diverted to deal with the breach, or having staff prevented from carrying out their day-to-day work. This compares to 41 per cent of primary schools, 65 per cent of secondary schools and 39 per cent of businesses.

2.2 Senior engagement with cyber security

The education institutions in our sample typically report a higher level of senior engagement with cyber security than the average UK business.

- Over nine in ten say that cyber security is a high priority for their governors or senior management (96% of the primary schools, 92% of the secondary schools and 91% of further and higher education institutions sampled). This is more in line with large businesses (95%) than with the average UK business (80%).
- Two-thirds or more update their governors or senior management on cyber security at least quarterly (65% of primary schools, 72% of secondary schools and 71% of further and higher education institutions, compared to 51% of businesses).
- Seven in ten or more have a governor or senior manager with responsibility for cyber security (76% of primary schools, 78% of secondary schools and 69% of further and higher education institutions, compared with 37% of businesses). Again, this is much closer to the large business result (68%).

2.3 Sources of information and guidance

The most common sources of information and guidance for education institutions are:

- their external cyber security or IT providers (40% of primary schools, 35% of secondary schools and 54% of further and higher education institutions)
- any government or public sector sources, including government websites, regulators and other public bodies (31%, 25% and 43% respectively).

For the further and higher education institutions in our sample, the greatest source of government guidance is the National Cyber Security Centre (noted by 31%). This is not the case for primary schools (no mentions) or secondary schools (2%). The highest specific public sector organisations mentioned among these groups is the Local Authority (by 23% of primary schools and 14% of secondary schools).

There are still large parts of our samples that have not heard of the various government initiatives and communications campaigns on cyber security:

- A total of 60% of primary schools, 67% of secondary schools and 46% of further and higher education institutions do not recall hearing of the Cyber Aware campaign.[2]
- Awareness of both the 10 Steps to Cyber Security[3] (77%) and Cyber Essentials[4] (86%) is extremely widespread in our further and higher education institution sample. However, awareness is much lower among primary schools (35% and 14% aware of each respective initiative) and secondary schools (29% and 39%).

2.4 Identifying cyber security risks

Almost all the education institutions surveyed have taken at least one of the actions shown in Figure 2.3 in the last 12 months, to help identify cyber security risks. This is a higher rate than

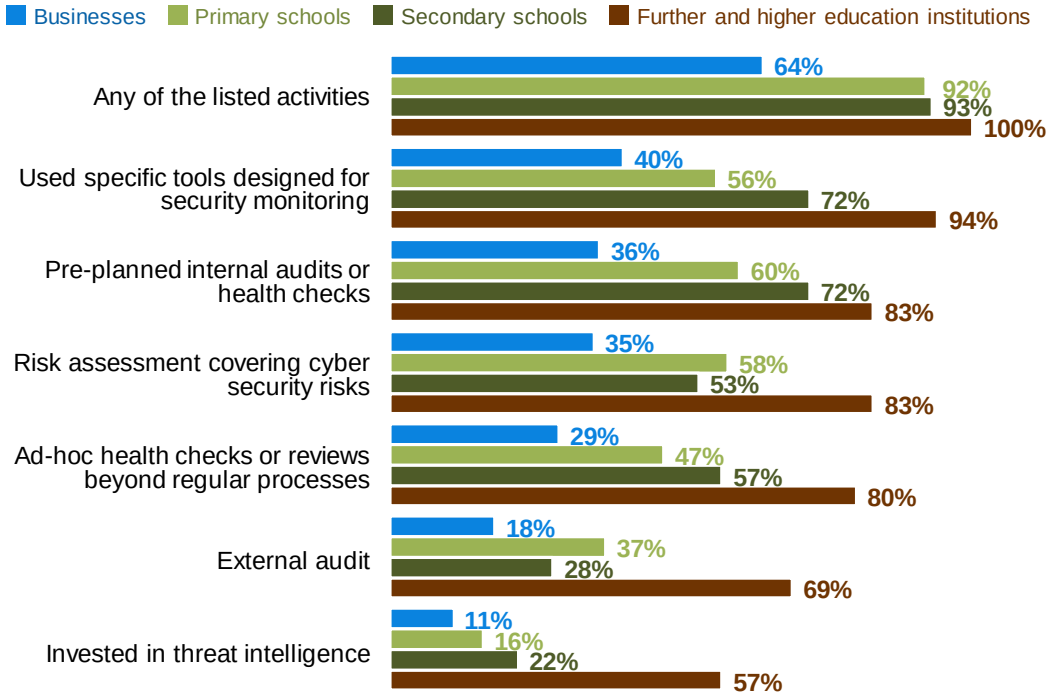
[2] See www.cyberaware.gov.uk.

[3] The 10 Steps to Cyber Security guidance, which aims to summarise what organisations should do to protect themselves. See https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security.

[4] The government-endorsed Cyber Essentials scheme, which enables organisations to be certified independently for having met a good-practice standard in cyber security. See https://www.cyberessentials.ncsc.gov.uk/.

for UK businesses (64%). The further and higher education institutions in our sample tend to have a more diverse range of activities, including external audits and using threat intelligence.

Figure 2.3: Percentage of education institutions that have carried out the following activities to identify cyber security risks in the last 12 months



Bases: 1,348 UK businesses; 108 primary schools; 72 secondary schools; 35 further and higher education institutions

All types of education institutions in our sample are also more likely than businesses to say they have reviewed supplier-related risks to cyber security, although this still appears to be an uncommon activity on balance for schools.

- Around a third of primary schools (34%) and secondary schools (36%) have reviewed the risks from their immediate suppliers, versus three-fifths of further and higher education institutions (60%). This compares to 15 per cent of businesses.
- Across the board, few have reviewed risks presented by their wider supply chains (24% of primary schools, 19% of secondary schools and 26% of further and higher education institutions, compared to 9% of businesses).

2.5 Approaches for managing cyber security risks

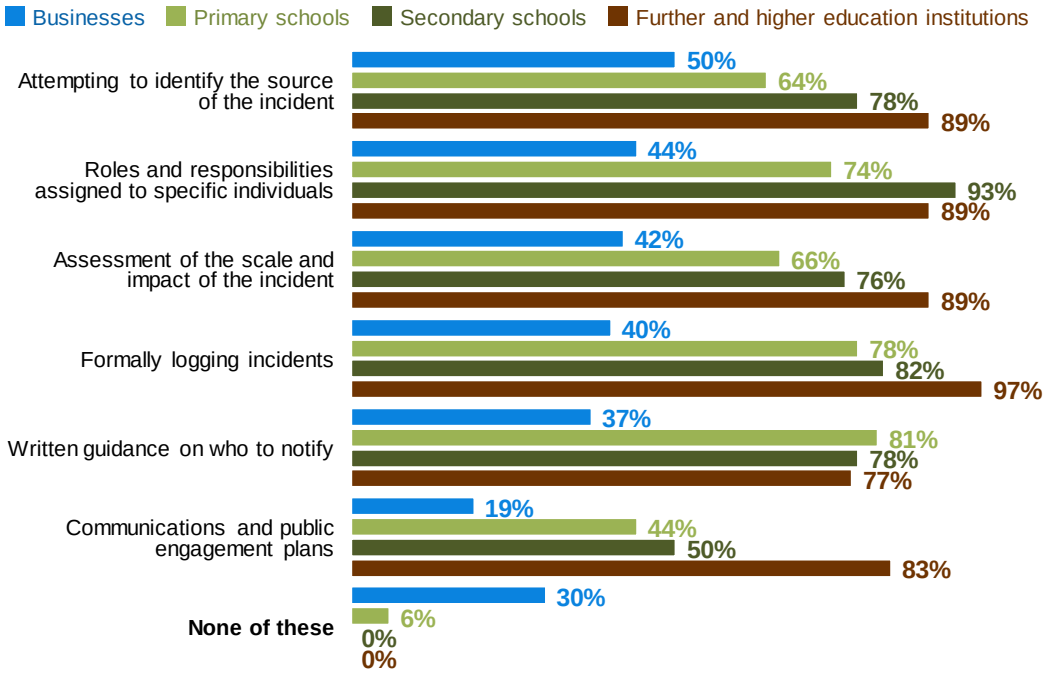
Governance approaches

Almost all secondary schools (92%) and further and higher education institutions (97%) have a cyber security policy. This figure is also high in primary schools relative to the UK business population (80%, vs. 38% of all businesses and 77% or large businesses) – although this does indicate that a sizeable minority of primary schools probably does not formally document their approach to cyber security at a central level.

Possibly related to this, our sample suggests that outsourcing cyber security is possibly more common among primary schools than other educational institutions. A total of 89 per cent of the primary schools we surveyed say an external provider manages their cyber security for them (vs. 53% of secondary schools and just 6 per cent of further and higher education institutions).

In the case of cyber security breaches, the primary schools in our sample tend to have slightly less developed incident response plans, as Figure 2.4 suggests. They are less likely than other education institutions to have roles and responsibilities assigned to specific individuals, and less likely to have communications plans. It is, nonetheless, worth noting that these results put primary schools on a par with the typical large business, while other education institutions seem to be further ahead than most large businesses in their governance processes.

Figure 2.4: Percentage of education institutions that take the following actions, or have these measures in place, for when they experience a cyber security incident



Bases: 1,348 UK businesses; 108 primary schools; 72 secondary schools; 35 further and higher education institutions

Insurance

Around half of further and higher education institutions (51%) report being insured against cyber risks, with a smaller proportion of primary schools (31%) and secondary school (26%) reporting this. It is worth noting that around half of the individuals in cyber roles that we surveyed in primary and secondary schools did not know whether their school had this kind of insurance (48% and 53% respectively).[5]

Technical rules and controls

We cover the range of technical rules and controls that education institutions have in place to help minimise the risk of cyber security breaches (Figure 2.5). Many of these are basic good practice controls taken from government guidance for the 10 Steps to Cyber Security or the Cyber Essentials scheme – which most of our sampled institutions purport to have seen.

We find, overwhelmingly, that the education institutions in our sample have technical rules or controls covering the five technical areas laid out in the Cyber Essentials guidance: boundary

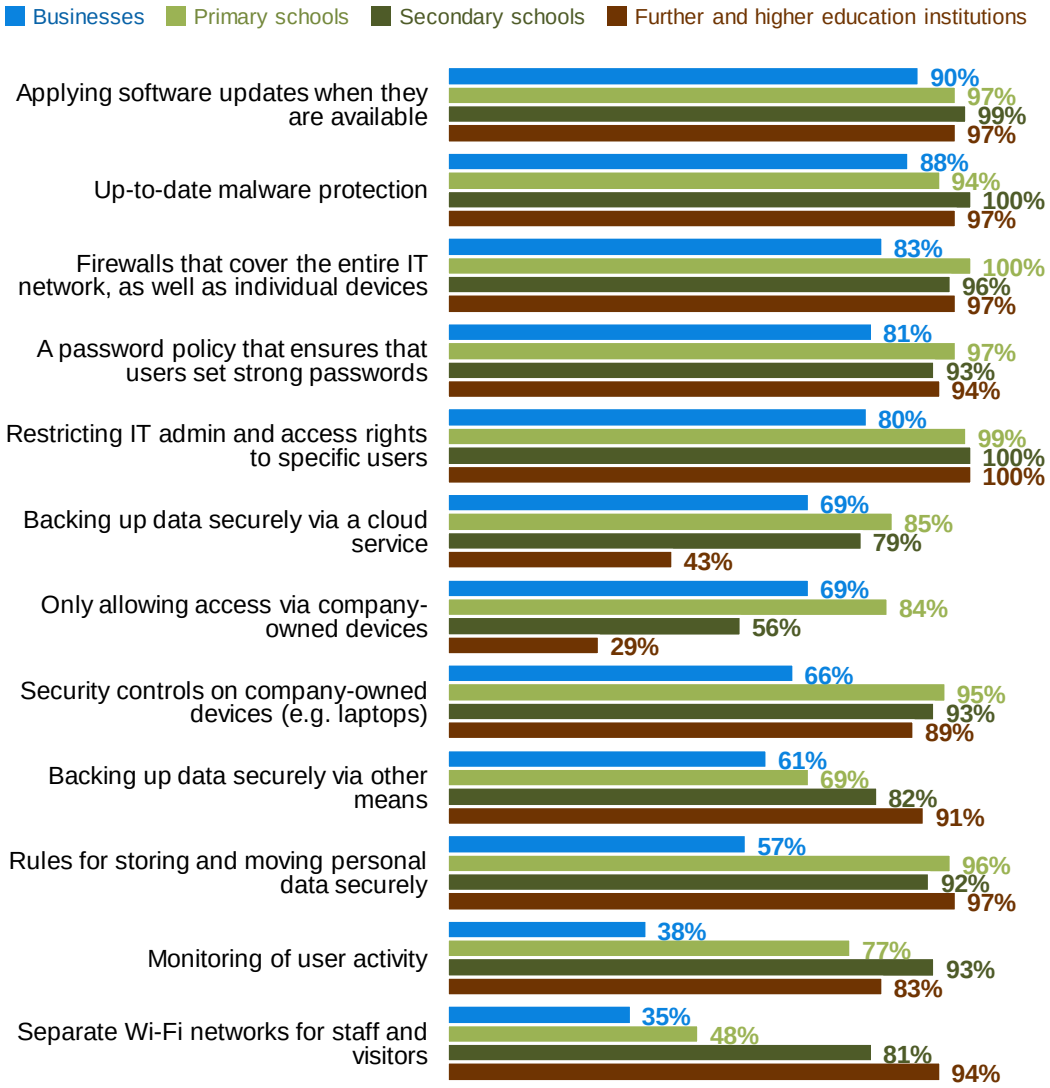
[5] Our interviewers sought to interview the senior person with most responsibility for cyber security within an organisation. This individual was identified by the organisation for us.

firewalls and internet gateways, secure configurations, user access controls, malware protection, and patch management (applying software updates).

In our sample, primary schools are less likely than other education institutions to have guest Wi-Fi networks. This may reflect the nature of their activities – dealing with young children who would not typically be allowed their own internet access at school – but could also represent a less considered risk for this group.

It is also notable that cloud back-ups are much less common in our further and higher education sample than in other education institutions.

Figure 2.5: Percentage of education institutions that have the following rules or controls in place



Bases: 1,348 UK businesses; 108 primary schools; 72 secondary schools; 35 further and higher education institutions

Implementing the 10 Steps to Cyber Security

Many of the technical rules and controls, as well as the other risk identification and risk management processes recorded in the survey can be directly mapped to the 10 Steps to Cyber Security guidance. The following table lays out these 10 Steps and how we have mapped them to our survey questions.

Table 2.1: Percentage of education institutions undertaking action in each of the 10 Steps areas

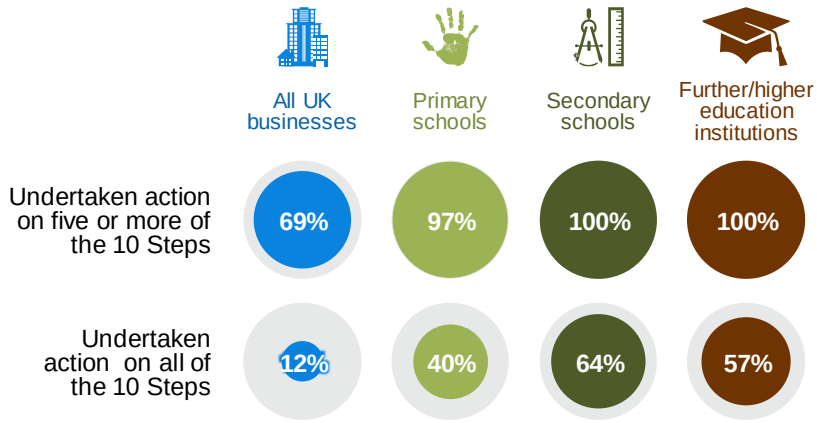
	Step description – *and how derived from the survey*	Businesses	Primary	Secondary	Further/ higher
1	Information risk management regime – *formal cyber security policies and the board are kept updated on actions taken*	35%	76%	82%	83%
2	Secure configuration – *organisation applies software updates when they are available*	90%	97%	99%	97%
3	Network security – *network firewalls*	83%	100%	96%	97%
4	Managing user privileges – *restricting IT admin and access rights to specific users*	80%	99%	100%	100%
5	User education and awareness – *formal policy covers what staff are permitted to do on the organisation's IT devices*	30%	70%	86%	97%
6	Incident management – *any incident management process*	68%	94%	99%	100%
7	Malware protection – *up-to-date malware protection*	88%	94%	100%	97%
8	Monitoring – *monitoring user activity or using security monitoring tools*	57%	85%	96%	97%
9	Removable media controls – *policy covers what can be stored on removable devices*	23%	63%	81%	69%
10	Home and mobile working – *policy covers remote or mobile working*	25%	60%	78%	86%

This table shows that the areas that are relatively less well covered among the sampled education institutions are to do with:

- having an information risk management regime
- formal cyber security policies covering staff use of IT
- removable media controls
- remote or mobile working policies – which is likely to reflect that core teaching roles typically prohibit home working in primary and secondary schools.

Looking at these 10 Steps together, virtually all education institutions have taken action on at least five of these steps, but there is still a way to go before these institutions have taken action in all 10 areas as demonstrated in Figure 2.6.

Figure 2.6: Percentage of education institutions that have undertaken action in half or all the 10 Steps guidance areas



Bases: 1,348 UK businesses; 108 primary schools; 72 secondary schools; 35 further and higher education institutions

Appendix A: Further information

1. The Department for Digital, Culture, Media and Sport would like to thank the following people for their work in the development and carrying out of the survey and for their work compiling this report.

    - Harry Williams, Ipsos MORI
    - Lydia Clark, Ipsos MORI
    - Catherine Crick, Ipsos MORI
    - Jayesh Navin Shah, Ipsos MORI

2. The Cyber Security Breaches Survey was first published in 2017 as a research report, and became an Official Statistic in 2018. The previous reports can be found at https://www.gov.uk/government/collections/cyber-security-breaches-survey. This includes the full report, infographics and the technical and methodological information for each year. The next version of the Cyber Security Breaches Survey is expected to be published in 2021.

3. The responsible DCMS analyst for this release is Emma Johns. The responsible statistician is Rishi Vaidya. For enquiries on this release, please contact Rishi on 020 7211 2320 or evidence@culture.gov.uk.

4. For general enquiries contact:

    Department for Digital, Culture, Media and Sport
    100 Parliament Street
    London
    SW1A 2BQ

    Telephone: 020 7211 6000

5. DCMS statisticians can be followed on Twitter via @DCMSInsight.

6. The Cyber Security Breaches Survey is an Official Statistics publication and has been produced to the standards set out in the Code of Practice for Official Statistics. For more information, see https://www.statisticsauthority.gov.uk/code-of-practice/. Details of the pre-release access arrangements for this dataset have been published alongside this release.

7. This work was carried out in accordance with the requirements of the international quality standard for Market Research, ISO 20252, and with the Ipsos MORI Terms and Conditions which can be found at http://www.ipsos-mori.com/terms.

Department for Digital, Culture, Media & Sport

4th Floor
100 Parliament Street
London
SW1A 2BQ